STATEMENT OF

MR. MATTHEW E. BRODERICK
DIRECTOR
HOMELAND SECURITY OPERATIONS CENTER

BEFORE THE
HOUSE COMMITTEE ON HOMELAND SECURITY
INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT SUBCOMMITTEE
JULY 20, 2005

Introduction

Good morning, Chairman Simmons, Representative Lofgren, and distinguished members of the Committee. It is my privilege to come before you today to discuss the primary ways the Department of Homeland Security (DHS) shares information through its Operations Center and the Homeland Security Information Network.

Homeland Security Operations Center (HSOC)

The Homeland Security Operations Center (HSOC) is a standing 24/7, interagency organization that is the national-level hub for domestic situational awareness and operational coordination pertaining to the prevention of terrorist attacks and domestic incident management. The HSOC facilitates homeland security information sharing and operational coordination with other Federal, State, local, tribal, and private sector organizations. It comprises over 35 Federal, State, and local government agencies.

The HSOC has three primary missions:

- Daily receipt and reporting of information from all available sources on suspicious activity, throughout the United States
- Incident management during catastrophic events within the United States
- Domestic situational awareness and development of common operating picture

Currently, DHS has the lead for controlling U.S. borders and ports of entry. The HSOC's day-to-day responsibilities include identification of possible terrorist threats to the Nation by collecting and reporting suspicious activities on who or what is approaching, attempting to cross, or residing within our borders. Collection and reporting of that information is shared with the entire Intelligence Community (IC), with a primary focus of providing information to the FBI, the National Counter Terrorism Center (NCTC), and the Office of Information Analysis (IA) within the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate. Those entities, rather than the HSOC, perform the intelligence analysis function. The information also is shared with other appropriate Federal, State, and local agencies, as well as with the private sector, primarily via the Homeland Security Information Network, which I will address momentarily.

The most critical element of the daily information gathering and refinement cycle is sharing the information gathered with IA, which then passes on possible threats to the Office of Infrastructure Protection. The HSOC follows a structured timeline throughout the course of the day. Beginning at midnight, DHS organizational components submit daily situational reports that are collected and vetted by the HSOC prior to being passed on for analysis. This provides a cursory first screening of information to avoid an inefficient use of IC analytical resources. This information also serves as material for the Secretary's morning brief and for the interagency Secure Video Teleconferencing (SVTC) that takes place twice daily. A product called the Homeland Security Operations Morning Brief, comprised of mostly suspicious activity reports

minus any information on U.S. persons contained within criminal intelligence protected by privacy laws, is shared on a Sensitive but Unclassified (SBU) level with about 1500 Federal, State, and local intelligence and law enforcement agencies and subscribers. In the morning and afternoon, a SVTC occurs with NCTC as chair and other members of the intelligence community. Information obtained the day before is discussed and shared as are requests for specific actions. DHS has been able to provide new insight and visibility into this process with its reports on who is entering, or trying to enter our borders; information, which in past years, would have been stove piped within individual agency data bases. Midmorning, all agencies within the HSOC meet and an intelligence brief is shared with all representatives and they are encouraged to share this information with their respective agencies. At the end of each day, HSOC-generated items are closed out or passed forward, if appropriate, and the cycle begins again.

As stated in the National Response Plan (NRP), another core mission of the HSOC is to serve as the national-level hub for information sharing during catastrophic events within the United States. It is also the primary conduit to the White House and the Secretary of Homeland Security for domestic situational awareness. Sharing of information and operational coordination is conducted through Emergency Operations Centers (EOC) at Federal, State, local, tribal, and regional levels, with the State Governors and their Homeland Security Advisors, as well as in relevant format with the private sector. During these incidents, situational awareness is also passed to the Inter-agency Incident Management Group (IIMG).

The IIMG, comprised of subject matter experts at the Assistant Secretary and Senior Government Executive level from most Federal agencies, is established within the HSOC. The IIMG provides strategic level recommendations and courses of action, prior to and/or during a catastrophic event, for consideration by the Secretary and other senior officials. In order to allow these representatives the time to focus on courses of action and recommendations, the IIMG members have reciprocal desk officers within the HSOC to provide them with continuous situational awareness and for requests for information.

The HSOC is also responsible for monitoring special events. These events come in five levels dependent upon the situation participants and estimated crowd number. The five levels and examples are:

National Special Security Events (NSSEs): Inaugurations, etc
Level 1: New Years Eve in New York City
Level 2: World Series
Level 3: Kentucky Derby
Level 4: Local Events

In each case, the HSOC offers senior watch officers to support major events in other cities or helps local officials “plug in” to national level intelligence and information sharing as it pertains to their particular event.

The Homeland Security Information Network (HSIN)

The Homeland Security Information Network (HSIN) is the primary conduit through which DHS shares information on domestic terrorist threats, suspicious activity reports, and incident management between and among all DHS stakeholders. It is set of tools and data sources that support DHS customers defined as users within multiple communities of interest (COI). It also provides collaboration and information sharing while enabling the stakeholder organization to determine the information and communications streams of value to its needs. The HSIN is a capability that provides secure and protected, real-time interactive connectivity among users at all levels of government, critical sectors and private industry with the HSOC.

The HSIN directly supports the Department's strategic goals to identify and understand threats, assess vulnerabilities; determine potential impacts and disseminate timely information to our homeland security partners and the American public; and detect, deter, and mitigate threats to our homeland. Specifically, it is designed to allow users to gather and fuse all terrorism-related intelligence; analyze and coordinate access to information related to potential terrorists and other threats; develop timely, actionable, and valuable information based on intelligence analysis and vulnerability assessments; ensure quick and accurate dissemination of relevant intelligence information to homeland security partners, including the public; and provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism, and other illegal activities.

HSIN is a user-friendly system. It enables Federal, State, territorial, local, international, tribal and private sector users to communicate and share information both with each other and with DHS in a real-time, secure and protected Web-based environment. This system provides participants direct access to an extensive suite of functions: mapping, a robust search engine/library, instant messaging and chat (collaboration) and an information-posting capability which interfaces with both DOJ's Law Enforcement Online (LEO) and the Regional Information Sharing System (RISS) networks. We currently have tens of thousands of users and we project to have hundreds of thousands of users by FY07.

Currently, the HSIN Communities of Interests include:

- HSIN Counter Terrorism (HSIN-CT): the common portal for all Federal, State, territorial, tribal, and local government agencies to share information relating to counter-terrorism and incident management
- Law Enforcement (JRIES LE-A): for law enforcement agencies that have major intelligence analysis departments (~150 or more members)
- Law Enforcement (LE): for all agencies dealing with LE Sensitive data (F/S/L) that meet the DOJ definition of Law Enforcement Sensitive
- Emergency Management (EM): for Federal, State, tribal, and local levels (local refers to county/major city) emergency operations centers to deal with major incidents
- HSIN Intelligence: being set up for use by the internal DHS intelligence community
- HSIN International: allows for rapid dialog between the HSOC and Canada, the United Kingdom, and Australia during a crisis

- HSIN SECRET: an immediate, inexpensive, and temporary approach to reach State and local homeland security and law enforcement sites that can receive Secret level information, pending full deployment in fiscal year 2007 of a new DHS Secret backbone called HSDN

Critical Infrastructure Warning Information Network (CWIN)
The Critical infrastructure Warning Information Network (CWIN) is a Federal government-operated network within HSIN that provides mission-critical, yet survivable, connectivity. CWIN Communities of Interest, include:

- Entities in the private sector vital to restoring the nation's critical infrastructures(e.g., electrical, information technology, and telecommunications)
- Entities in the Federal and State government, vital to maintain government-wide connectivity with DHS; sector-specific agencies and resources; State Homeland Security Advisors; and Emergency Management Centers.

Most importantly, CWIN provides survivable DHS capability for information sharing and collaboration for critical infrastructure restoration when primary forms of communication such as the Internet and Public Switched Telephone Network (PSTN) are inoperable because it is not dependent on the public internet or PSTN. CWIN is used routinely for testing and exercises as well as information sharing to ensure operational readiness when the need arises.

HSIN Critical Infrastructure (HSIN-CI)
The HSIN-CI program was designed, implemented, and deployed as a DHS-directed and regionally coordinated private and public self-governing program, with a vetted audience (approximately 40,000 members, 90% private sector) for national, regional, and local information sharing and all hazards, 24/7 alerts and warnings. The technology to support the program field operations was installed in the secured facilities of the FEMA Regional District Offices in FEMA regions IV, V, VI, and X. Participation includes private and public members from the 19 states within these regions and, because the program uses the Internet, HSIN-CI has membership from all 50 states.

The HSIN-CI program is administered through Regional Managers from the FBI's Field Intelligence Groups, at the direction of the HSOC. CI members nationwide promote the HSIN-CI program within their areas of expertise, creating a self-administered and vetted private and public membership built upon existing relationships and communication lines that is locally administered and governed in coordination with DHS (HSOC). Public notification options in HSIN-CI include two-way voice and short message service (SMS) messaging based on current location and/or proximity to an event, and a publicly available collection of suspicious activity reports. HSIN-CI members can submit reports, as well as receive sector/location-specific information from submitted reports.

HSIN Critical Sector (HSIN-CS)
HSIN-CI is designed to enhance the protection, preparedness, and crisis communication and coordination capabilities of the nation's 17 critical infrastructure and key resource sector owners and operators, HSIN-CS is primarily a mechanism for information sharing and collaboration within each specific critical infrastructure sector and the Federal government.

The following is the list of Critical Infrastructures and Key Resources, as defined by HSPD-7: Agriculture and Food, Public Health/Health Care, Drinking Water and Waste Water Treatment Systems, Energy, Banking and Finance, National Monuments and Icons, Defense Industrial Base, Information Technology, Telecommunications, Chemical, Transportation Systems, Emergency Services, Postal and Shipping, Government Facilities, Dams, Commercial Facilities, Nuclear Reactors, Materials, and Waste

HSIN/US Computer Emergency Response Team (HSIN/US-CERT)
This is the focal point for addressing cyber security incidents within the federal government. The portal is an information dissemination mechanism to communicate relevant cyber information. Using a suite of tools such as secure messaging, forms, secure chat rooms, alerts, and shared libraries, US-CERT pushes necessary information to a broad or targeted audience, as required.

HSIN Current Status
The HSIN is operational in 50 States, the District of Columbia, five U.S. Territories, 53 major urban areas, Emergency Management Agencies, Homeland Security Advisors' Offices, Governors' Offices, State Law Enforcement Agencies, National Guard Centers, mayors of major cities, Emergency Operations Centers, and city law enforcement agencies. It is operational in three foreign countries: the United Kingdom, Canada, and Australia. HSIN SBU is currently being expanded at the state and local level through a pilot program involving 7-8 States in order to determine how the system can best be utilized within different governance structures. HSIN SECRET is being deployed and tested at 50 state EOCs and 18 additional State and local LE activities. There are pilot programs in 11 Information Sharing and Analysis Centers (Electric, Water, Food and Agriculture, Public Transit, Oil and Gas, Nuclear, Dams, Chemical, Postal, Nonprofit, and Health/Public Health). Plans are in place to begin deployment of a SECRET level component of HSIN to State and Local sites, and HSIN is being rolled out to all DHS component agencies.

HSIN has become a cornerstone of the Department's ability to communicate with homeland security partners and stakeholders across the nation. We will continue to build on our success as we extend connectivity to a wider user population and improve the tools availability for communication, collaboration and analysis of information.

This concludes my prepared remarks. I would be happy to answer any questions you may have at this time.

Annex A

HSOC Composition

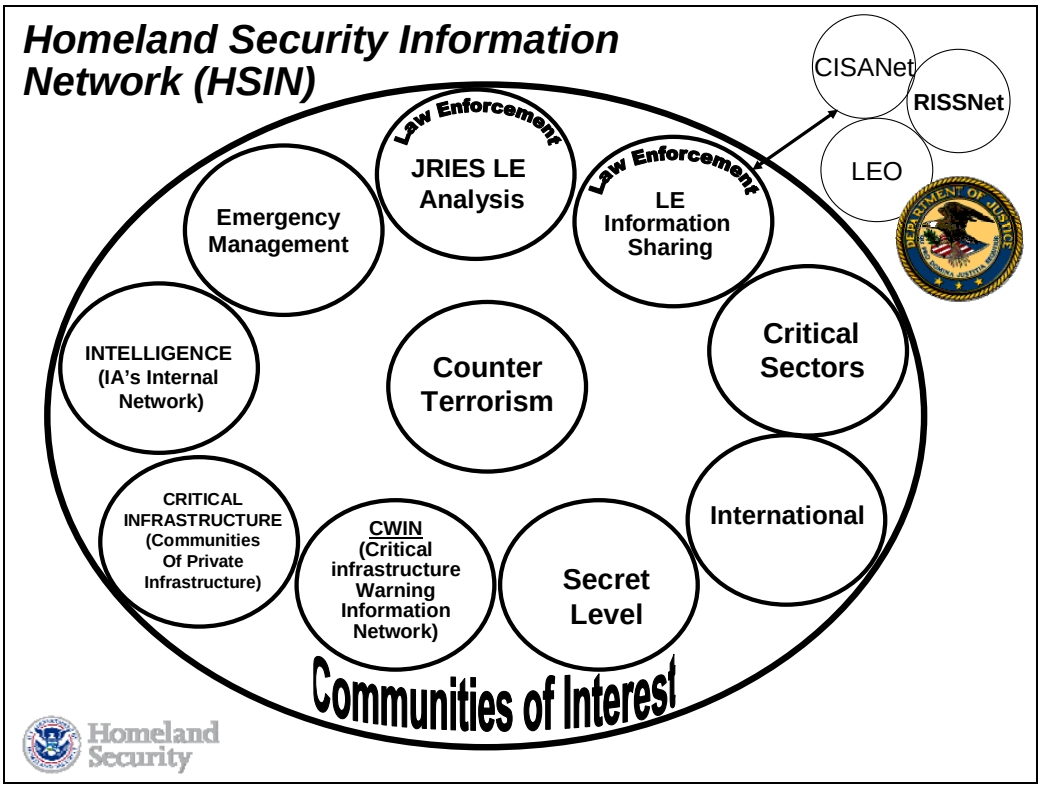
- **INTEL & INFRASTRUCTURE PROTECTION**
- **Central Intelligence Agency**
- **Defense Intelligence Agency**
- **National Security Agency**
- **National Geospatial Intelligence Agency**
- **Federal Bureau of Investigation**
- **Department of Interior (US Park Police)**
- **Drug Enforcement Administration**
- **Alcohol, Tobacco, and Firearms**
- **United States Secret Service**
- **Immigration Customs Enforcement**
- **Federal Protective Service**
- **Federal Air Marshal Service**
- **Transportation Security Administration**
- **Customs and Border Protection**
- **United States Coast Guard**
- **Department of Energy**
- **Department of State**
- **Department of Defense**
- **Department of Transportation**
- **Postal Inspection Service**
- **Environmental Protection Agency**
- **US Capitol Police**
- **DC Metro PD**
- **VA State Police**
- **Fairfax County PD**
- **LAPD**
- **NYPD**

- **INCIDENT MANAGEMENT**
- **Department of Veterans Affairs**
- **Department of Health and Human Services**
- **Federal Emergency Management Agency**
- **National Oceanic Atmospheric Administration**

- **OVERARCHING**
- **Border and Transportation Security**
- **State and Local Coordination Liaison**
- **Science and Technology Directorate**
- **Public Affairs**
- **Information Analysis Office**
- **Infrastructure Protection Office**
- **Geo-Spatial Mapping Office**

- **ON AN AS REQUIRED BASIS**
- **Nuclear Regulatory Commission**
- **US Department of the Treasury**

Annex B


Homeland Security Information Network (HSIN)
CISANet
RISSNet
LEO
Law Enforcement
JRIES LE Analysis
Law Enforcement
LE Information Sharing
Emergency Management
INTELLIGENCE (IA's Internal Network)
Counter Terrorism
Critical Sectors
CRITICAL INFRASTRUCTURE (Communities Of Private Infrastructure)
CWIN (Critical infrastructure Warning Information Network)
Secret Level
International
Communities of Interest
Homeland Security